



# Practical Software Diversification for WebAssembly

JAVIER CABRERA-ARTEAGA

Doctoral Thesis in Computer Science  
Supervised by  
Benoit Baudry and Martin Monperrus  
Stockholm, Sweden, 2023

TRITA-EECS-AVL-2020:4  
ISBN 100-

KTH Royal Institute of Technology  
School of Electrical Engineering and Computer Science  
Division of Software and Computer Systems  
SE-10044 Stockholm  
Sweden

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges  
till offentlig granskning för avläggande av Teknologie doktorexamen i elektroteknik  
i .

© Javier Cabrera-Arteaga , date

Tryck: Universitetsservice US AB

**Abstract**

**Keywords:** Lorem, Ipsum, Dolor, Sit, Amet

**Sammanfattning**

# LIST OF PAPERS

1. ***WebAssembly Diversification for Malware Evasion***  
**Javier Cabrera-Arteaga**, Tim Toady, Martin Monperrus, Benoit Baudry  
*Computers & Security, Volume 131, 2023, 17 pages*  
<https://www.sciencedirect.com/science/article/pii/S0167404823002067>
2. ***Wasm-mutate: Fast and Effective Binary Diversification for WebAssembly***  
**Javier Cabrera-Arteaga**, Nicholas Fitzgerald, Martin Monperrus, Benoit Baudry  
*Under review, 17 pages*  
<https://arxiv.org/pdf/2309.07638.pdf>
3. ***Multi-Variant Execution at the Edge***  
**Javier Cabrera-Arteaga**, Pierre Laperdrix, Martin Monperrus, Benoit Baudry  
*Moving Target Defense (MTD 2022), 12 pages*  
<https://dl.acm.org/doi/abs/10.1145/3560828.3564007>
4. ***CROW: Code Diversification for WebAssembly***  
**Javier Cabrera-Arteaga**, Orestis Floros, Oscar Vera-Pérez, Benoit Baudry, Martin Monperrus  
*Measurements, Attacks, and Defenses for the Web (MADWeb 2021), 12 pages*  
<https://doi.org/10.14722/madweb.2021.23004>
5. ***Superoptimization of WebAssembly Bytecode***  
**Javier Cabrera-Arteaga**, Shrinish Donde, Jian Gu, Orestis Floros, Lucas Satabin, Benoit Baudry, Martin Monperrus  
*Conference Companion of the 4th International Conference on Art, Science, and Engineering of Programming (Programming 2021), MoreVMs, 4 pages*  
<https://doi.org/10.1145/3397537.3397567>
6. ***Scalable Comparison of JavaScript V8 Bytecode Traces***  
**Javier Cabrera-Arteaga**, Martin Monperrus, Benoit Baudry  
*11th ACM SIGPLAN International Workshop on Virtual Machines and Intermediate Languages (SPLASH 2019), 10 pages*  
<https://doi.org/10.1145/3358504.3361228>



## ACKNOWLEDGEMENT



# Contents

<b>List of Papers</b>	<b>iii</b>
<b>Acknowledgement</b>	<b>v</b>
<b>Contents</b>	<b>1</b>
<b>I Thesis</b>	<b>3</b>
<b>1 Introduction</b>	<b>5</b>
1.1 Background . . . . .	5
1.2 Problem statement . . . . .	5
1.3 Automatic Software diversification requirements . . . . .	5
1.4 List of contributions . . . . .	5
1.5 Summary of research papers . . . . .	6
1.6 Thesis outline . . . . .	6
<b>2 Background and state of the art</b>	<b>7</b>
2.1 WebAssembly . . . . .	7
2.1.1 From source code to WebAssembly . . . . .	8
2.1.2 WebAssembly's binary format . . . . .	9
2.1.3 WebAssembly's runtime structure . . . . .	11
2.1.4 WebAssembly's control flow . . . . .	13
2.1.5 WebAssembly's ecosystem . . . . .	14
2.1.6 WebAssembly's binary analysis . . . . .	15
2.1.7 WebAssembly's security . . . . .	16
2.2 Software diversification . . . . .	17
2.2.1 Generating Software Diversification . . . . .	17
2.2.2 Variants generation . . . . .	17
2.2.3 Variants equivalence . . . . .	17
2.2.4 Defensive Diversification . . . . .	17

2.2.5	Offensive Diversification . . . . .	17
<b>3</b>	<b>Automatic Software Diversification for WebAssembly</b>	<b>19</b>
3.1	CROW: Code Randomization of WebAssembly . . . . .	20
3.1.1	Enumerative synthesis . . . . .	21
3.1.2	Constant inferring . . . . .	22
3.1.3	CROW instantiation . . . . .	23
3.2	MEWE: Multi-variant Execution for WebAssembly . . . . .	25
3.2.1	Multivariant generation . . . . .	26
3.3	WASM-MUTATE: Fast and Effective Binary for WebAssembly . . . . .	29
3.3.1	WebAssembly Rewriting Rules . . . . .	30
3.3.2	E-Graphs traversals . . . . .	31
3.3.3	WASM-MUTATE instantiation . . . . .	32
3.4	Comparing CROW, MEWE, and WASM-MUTATE . . . . .	34
3.4.1	Security applications . . . . .	37
3.5	Conclusions . . . . .	38
<b>4</b>	<b>Exploiting Software Diversification for WebAssembly</b>	<b>39</b>
4.1	Offensive Diversification: Malware evasion . . . . .	39
4.1.1	Threat model . . . . .	40
4.1.2	Approach . . . . .	41
4.1.3	Results . . . . .	42
4.2	Defensive Diversification: Speculative Side-channel protection . . . . .	43
4.2.1	Threat model . . . . .	43
4.2.2	Approach . . . . .	43
4.2.3	Results . . . . .	43
4.2.4	Partial input/output validation . . . . .	44
4.2.5	Some other works to be cited along with the paper. Mostly in the Intro . . . . .	44
4.3	Conclusions . . . . .	45
<b>5</b>	<b>Conclusions and Future Work</b>	<b>47</b>
5.1	Summary of technical contributions . . . . .	47
5.2	Summary of empirical findings . . . . .	47
5.3	Future Work . . . . .	47
<b>II</b>	<b>Included papers</b>	<b>49</b>
Superoptimization of WebAssembly Bytecode		53

CONTENTS	3
CROW: Code Diversification for WebAssembly	<b>55</b>
Multi-Variant Execution at the Edge	<b>57</b>
WebAssembly Diversification for Malware Evasion	<b>59</b>
Wasm-mutate: Fast and Effective Binary Diversification for WebAssembly	<b>61</b>
Scalable Comparison of JavaScript V8 Bytecode Traces	<b>63</b>



## **Part I**

# **Thesis**

